A - 1

Protokol Perjanjian Kunci Berdasarkan Masalah Konjugasi Pada Matriks Atas Lapangan Hingga

Agustin Rahayuningsih, M.Zaki Riyanto
Jurusan Matematika, Fakultas Sains dan Teknologi, UIN Sunan Kalijaga Yogyakarta
tintina_adja@yahoo.com

Abstrak−Protokol perjanjian kunci merupakan skema pengamanan pesan yang menggunakan kunci rahasia.Penggunaan kunci keamanan ketika berkomunikasi sangatlah penting, untuk menghindari penyadapan oleh pihak yang tidak diinginkan. Kunci rahasia digunakan pada proses enkripsi-dekripsi pesan yang dikirim atau diterima dalam kriptografi. Salah satu perjanjian kunci yang dikenal secara umum adalah perjanjian kunci Diffie-Hellman, yang didasarkan pada masalah logaritma diskrit suatu grup siklik.Protokol perjanjian Diffie-Hellman ini dapat dikembangkan pada grup non-komutatif dari matriks, yang entri-entrinya merupakan lapangan hingga atas polinomial untuk mendapatkan kunci rahasia.Kemudian kunci yang diperoleh diaplikasikan pada suatu komunikasi rahasia menggunakan sistem keamanan yaitu sistem kriptografi Cipher Hill.

***Kata Kunci : Sistem Cipher Hill, Protokol Perjanjian Kunci, Grup Non-Komutatif, Masalah Konjugasi, Lapangan Hingga*.**

I. PENDAHULUAN

A. Latar Belakang

Kriptografi merupakan suatu ilmu aljabar abstrak yang mempelajari teknik – teknik matematika yang berhubungan dengan aspek-aspek keamanan informasi seperti kerahasiaan (keamanan) data, keabsaan data, integritas data, serta autentikasi data. [1]Namun tidak semua keamanan informasi dapat diselesaikan dengan kriptografi, selain itu kriptografi dapat diartikan sebagai ilmu yang mempelajari berbagai teknik pengamanan pesan atau penyandian.

Hal penting yang dibutuhkan pada permasalahan komunikasi jarak jauh yaitu kunci rahasia, kunci rahasia yang digunakan hanya diketahui oleh kedua belah pihak dalam melakukan komunikasi yaitu untuk mengubah pesan asli menjadi suatu kode yang tidak dapat dimengerti orang lain atau pihak penyadap sehingga keamanan dapat terjaga.[2]

Penelitian mengenahi pembuatan kunci rahasia, diawali dari Algoritma kunci publik yang diterbitkan dalam sebuah makalah oleh Whitfield Diffie dan Martin Hellman pada tahun 1976, yang memperkenalkan konsep revolusiner kriptografi kunci publik dan memberikan metode baru untuk pertukaran kunci dengan tingkat keamanan berdasar pada kekuatan masalah diskret. Metode ini merupakan metode pertama untuk menciptakan sebuah kunci rahasia bersama antara dua belah pihak melalui sebuah jalur komunikasi yang tidak aman.[3]

Konsep pembuatan kunci menggunakan metode sederhana pada makalah Diffie-Hellman mulai dikembangkan lebih lanjut oleh beberapa penelitian, antara lain penelitian dari, Myasnikov, dkk (2008) yang menyelidiki suatu masalah konjugasi pada suatu grup non-komutatif, selanjutnya M.Zaki Riyanto (2012) meneliti penggunaan grup $GL_n(\mathbb{Z}_p)$ yaitu matriks atas lapangan $\mathbb{Z}_p$ dengan p adalah bilangan prima yang diterapkan pada permasalahan konjugasi dan Najib Mubarok (2013) yang menjelaskan konsep polinomialtak tereduksidalam pengamanan pesanrahasia.

Beberapa pembahasan yang dilakukan penelitian sebelumnya, penulis tertarik mengembangkan penelitian dari M.Zaki Riyanto (2012) yaitu menyelesaikan masalah komunikasi mengunakan kunci rahasia dengan konsep dasar masalah diskrit yang digunakan pada perjanjian protokol kunci berdasarkan pada masalah konjugasi atas matriks kunci dengan entri-entrinya berupa lapangan berhingga atas polinomial.

Lapangan hingga GF digunakan sebagai landasan keamanan dalam pembuatan kunci rahasia pada protokol perjanjian kunci, yang didefinisikan himpunan semua matriks berukuran *n* x *n* yang *invertibel* dan memiliki determinan tidak nol. Selain itu entri-entrinya berupa persamaan polinomial. Kunci rahasia yang diperoleh disepakati kedua pihak yang berkomunikasi guna mengamankan informasi rahasia. Selanjutnya disusun juga himpunan grup non-komutatif terhadap operasi perkalian matriks[4]

$$GL_n(p) = \{A \in M_n(p) | \det(A) \neq 0\}, n \geq 2\}$$

pada*plainteks* dan *chiperteks* diwakili oleh matriks *n* x 1, sehingga dibentuk fungsi untuk proses enkripsi dan dekripsi pesan.

II. HASIL DAN PEMBAHASAN

Dalam penelitian ini Alice dan Bob ingin melakukan komunikasi rahasia, di sini masalah yang muncul adalah bagaimana cara Alice mengirimkan pesan rahasia kepada Bob, sehingga tidak ada pihak yang tidak diinginkan mengetahui isi pesan tersebut?

Dari masalah yang muncul tersebut Alice dan Bob sepakat melakukan komunikasi rahasia menggunakan Sistem Kriptografi Cipher Hill, untuk menjaga keamanan Komunikasi, maka Alice dan Bob memilih menerapkan Sistem Keamanan Cipher Hill ke dalam Protokol Perjanjian Kunci berdasarkan masalah konjugasi yang kemudian memilih lapangan *GF* sebagai keamanan selanjutnya dalam entri-entri matriks.

Kemudian, proses pembuatan kunci diakhiri dengan membentuk sebuah matriks atas lapangan hingga dari $GF(p^m)$ yang dinotasikan dengan :

$$GL_n\big(GF(p^m)\big) = \{A \in M_n(GF(p^m)) | \det A \neq 0\}.$$

Kunci rahasia yang dibentuk berupa matriks bujur sangkar dengan beberapa syarat yaitu determinan tidak sama dengn nol, setiap entri pada matriks kunci merupakan elemen dari $GF(p^m)$.

Setelah itu diilakukan proses pertukaran kunci, berikut skema pertukaran kunci

Alice dan Bob mempublikasikan grup non-komutatif $GF(2^4)/ < x^4 + x + 1 >$ dan memilih :

$$w = \begin{bmatrix} x^2 & x \\ 1 & x \end{bmatrix} \in GL_2(GF(p^4)), \text{ dan } H = \left\{ \begin{bmatrix} a & b \\ b & a \end{bmatrix} | a, b \in GL(p^4) \right\}$$

Alice	Bob
1. Alice memilih secara rahasia $r = \begin{bmatrix} x & 1 \\ 1 & x \end{bmatrix} \in H$ 2. Alice menghitung $m = r^{-1}wr$ $= \begin{bmatrix} x^2+1 & x^3+x+1 \\ x^3+x+1 & x^2+1 \end{bmatrix}$ $\begin{bmatrix} x^2 & x \\ 1 & x \end{bmatrix}\begin{bmatrix} x & 1 \\ 1 & x \end{bmatrix} \bmod x^4+x+1$ $= \begin{bmatrix} x^2 & 1 \\ x & x \end{bmatrix}$ 3. Alice mengirimkan *m* kepada Bob. 4. Alice menerima *n* dari Bob 5. Alice menghitung $K_1 = r^{-1}nr$ $K_1 = \begin{bmatrix} x^2+1 & x^3+x+1 \\ (x^3+x+1) & x^2+1 \end{bmatrix}\begin{bmatrix} x^2 & 1 \\ x & x \end{bmatrix}$ $\begin{bmatrix} x & 1 \\ 1 & x \end{bmatrix} \bmod x^4+x+1$ $K_1 = \begin{bmatrix} x^2 & x \\ 1 & x \end{bmatrix}$	1. Bob memilih secara rahasia $s = \begin{bmatrix} x^2 & x \\ x & x^2 \end{bmatrix} \in H$ 2. Bob menghitung $n = s^{-1}ws$ $= \begin{bmatrix} x^3+x+1 & (x^3+x^2) \\ (x^3+x^2) & x^3+x+1 \end{bmatrix}$ $\begin{bmatrix} x^2 & x \\ 1 & x \end{bmatrix}\begin{bmatrix} x^2 & -x \\ x & x^2 \end{bmatrix} \bmod x^4+x+1$ $= \begin{bmatrix} x^2 & 1 \\ x & x \end{bmatrix}$ 3. Bob mengirimkan *n* kepada Alice. 4. Bob menerima *m* dari Alice 5. Bob menghitung $K_2 = s^{-1}ms$ $K_2 = \begin{bmatrix} x^3+x+1 & (x^3+x^2) \\ (x^3+x^2) & x^3+x+1 \end{bmatrix}\begin{bmatrix} x^2 & 1 \\ x & x \end{bmatrix}$ $\begin{bmatrix} x^2 & x \\ x & x^2 \end{bmatrix} \bmod x^4+x+1$ $K_2 = \begin{bmatrix} x^2 & x \\ 1 & x \end{bmatrix}$

Alice dan Bob mendapatkan kunci rahasia yang sama yaitu Alice mendapatkan kunci rahasia $K=K_1=K_2=\begin{bmatrix} x^2 & x \\ 1 & x \end{bmatrix}$

Enkripsi

Langkah selanjutnya, Alice mengenkripsikan pesan rahasianya, proses enkripsi merupakan proses pemetaan dari plainteks menjadi cipherteks. Pada proses enkripsi ini Alice akan menggunakan tabel ASCII, pada setiap chiperteks akan dibagi kedalam 4 bit

Kemudian, Alice membagi ASCII Biner setiap 4 bit untuk mendapatkan plainteks yang lebih sederhana. Berikut pembagian setiap plainteks-plainteks:

X_1 =B$\leftrightarrow \begin{bmatrix} 0100 \\ 0010 \end{bmatrix} \leftrightarrow \begin{bmatrix} x^2 \\ x \end{bmatrix}$

X_2 =E$\leftrightarrow \begin{bmatrix} 0100 \\ 0101 \end{bmatrix} \leftrightarrow \begin{bmatrix} x^2 \\ x^2+1 \end{bmatrix}$

X_3 =L $\leftrightarrow \begin{bmatrix} 0100 \\ 0000 \end{bmatrix} \leftrightarrow \begin{bmatrix} x^2 \\ 0 \end{bmatrix}$

X_4 = I $\leftrightarrow \begin{bmatrix} 0100 \\ 1001 \end{bmatrix} \leftrightarrow \begin{bmatrix} x^2 \\ x \end{bmatrix}$

X_5 = E $\leftrightarrow \begin{bmatrix} 0100 \\ 0101 \end{bmatrix} \leftrightarrow \begin{bmatrix} x^2 \\ x^2+1 \end{bmatrix}$

X_6 = V $\leftrightarrow \begin{bmatrix} 0101 \\ 0110 \end{bmatrix} \leftrightarrow \begin{bmatrix} x^2+1 \\ x \end{bmatrix}$

X_7 = E$\leftrightarrow \begin{bmatrix} 0100 \\ 0101 \end{bmatrix} \leftrightarrow \begin{bmatrix} x^2 \\ x^2+1 \end{bmatrix}$

Plainteks-plainteks yang didapat selanjutnya digunakan pada proses enkripsi yaitu $e_k = K.X_i = Y_i$ untuk mendapatkan chiperteks yang akan dikirimkan kepada Bob, yaitu sebagai berikut :$e_{k1}(X_1) = KX_1 \leftrightarrow \begin{bmatrix} x^2 & x \\ 1 & x \end{bmatrix} \begin{bmatrix} x^2 \\ x \end{bmatrix} mod\ x^4+x+1$

$= \begin{bmatrix} x^2+x+1 \\ 0 \end{bmatrix} \leftrightarrow \begin{bmatrix} 0111 \\ 0000 \end{bmatrix}$

$e_{k_2}(X_2) = KX_2 \leftrightarrow \begin{bmatrix} x^2 & x \\ 1 & x \end{bmatrix} \begin{bmatrix} x^2 \\ x^2+1 \end{bmatrix} mod\ x^4+x+1$

$= \begin{bmatrix} x^3+1 \\ x^3+x^2+x \end{bmatrix} \leftrightarrow \begin{bmatrix} 1001 \\ 1110 \end{bmatrix}$

$e_{k_3}(X_3) = KX_3 \leftrightarrow \begin{bmatrix} x^2 & x \\ 1 & x \end{bmatrix} \begin{bmatrix} x^2 \\ 0 \end{bmatrix} mod\ x^4+x+1$

$= \begin{bmatrix} x^3 \\ x^3+x^2+x+1 \end{bmatrix} \leftrightarrow \begin{bmatrix} 1000 \\ 1111 \end{bmatrix}$

$e_{k_4}(X_4) = KX_4 \leftrightarrow \begin{bmatrix} x^2 & x \\ 1 & x \end{bmatrix} \begin{bmatrix} x^2 \\ x \end{bmatrix} mod\ x^4+x+1$

$= \begin{bmatrix} x \\ x+1 \end{bmatrix} \leftrightarrow \begin{bmatrix} 0010 \\ 0011 \end{bmatrix}$

$e_{k_5}(X_5) = KX_5 \leftrightarrow \begin{bmatrix} x^2 & x \\ 1 & x \end{bmatrix} \begin{bmatrix} x^2 \\ x^2+1 \end{bmatrix} mod\ x^4+x+1$

$= \begin{bmatrix} x^3+1 \\ x^3+x^2+x \end{bmatrix} \leftrightarrow \begin{bmatrix} 1001 \\ 1110 \end{bmatrix}$

$e_{k_6}(X_6) = KX_6 \leftrightarrow \begin{bmatrix} x^2 & x \\ 1 & x \end{bmatrix} \begin{bmatrix} x^2+1 \\ x \end{bmatrix} mod\ x^4+x+1$

$$= \begin{bmatrix} x^3+x^2+1 \\ x^3+1 \end{bmatrix} \leftrightarrow \begin{bmatrix} 1101 \\ 1001 \end{bmatrix}$$

$$e_{k_7}(X_7) = KX_7 \leftrightarrow \begin{bmatrix} x^2 & x \\ 1 & x \end{bmatrix} \begin{bmatrix} x^2 \\ x^2+1 \end{bmatrix} mod\ x^4+x+1$$

$$= \begin{bmatrix} x^3+1 \\ x^3+x^2+x \end{bmatrix} \leftrightarrow \begin{bmatrix} 1001 \\ 1110 \end{bmatrix}$$

Cipherteks yang diperoleh, selanjutnya akan dikirimkan kepada Bob yaitu : 01110000-10011110-10001111-00100101-10011110-11011001-10011110

Dekripsi

Proses selanjutnya yang dilakukan Bob adalah mendekripsikan pesan yang diterima dari Alice yaitu: "01110000-10011110-10001111-00100101-10011110-11011001-10011110 " , melalui proses dekripsi, dimana pesan yang diterima berupa chiperteks yang diterjemahkan dengan invers dari Kunci yang telah diperoleh. Proses di rumuskan sebagai berikut :$d_k = K^{-1}Y = X$.

K= $\begin{bmatrix} x^2 & x \\ 1 & x \end{bmatrix}$, maka untuk

$$K^{-1} = \begin{bmatrix} x^2 & x \\ 1 & x \end{bmatrix}^{-1} mod\ x^4+x+1 = \begin{bmatrix} x^3+x+1 & x^3+x+1 \\ x^3+x^2 & x^2+1 \end{bmatrix} \leftrightarrow \begin{bmatrix} 1011 & 1011 \\ 1100 & 0101 \end{bmatrix}$$

Setelah menghitung invers dari matriks kunci maka Bob membentuk bloks-bloks pesan ke dalam matriks. Berikut bloks-bloks yang dibentuk oleh Bob :$\begin{bmatrix} 0111 \\ 0000 \end{bmatrix}, \begin{bmatrix} 1001 \\ 1110 \end{bmatrix}, \begin{bmatrix} 1000 \\ 1111 \end{bmatrix}, \begin{bmatrix} 0010 \\ 0011 \end{bmatrix}, \begin{bmatrix} 1001 \\ 1110 \end{bmatrix}, \begin{bmatrix} 1101 \\ 1001 \end{bmatrix}, \begin{bmatrix} 1001 \\ 1110 \end{bmatrix}$

Berikut proses dekripsi yang dilakukan Bob setelah membentuk bloks-bloks chiperteks :

$d_{k_1}(Y_1) = K^{-1}Y_1$

$$= \begin{bmatrix} x^3+x+1 & x^3+x+1 \\ x^3+x^2 & x^2+1 \end{bmatrix} \begin{bmatrix} x^2+x+1 \\ 0 \end{bmatrix} mod\ x^4+x+1$$

$$= \begin{bmatrix} x^2 \\ x \end{bmatrix} \leftrightarrow \begin{bmatrix} 0100 \\ 0010 \end{bmatrix} \leftrightarrow B$$

$d_{k_2}(Y_2) = K^{-1}Y_2$

$$= \begin{bmatrix} x^3+x+1 & x^3+x+1 \\ x^3+x^2 & x^2+1 \end{bmatrix} mod\ x^4+x+1$$

$$= \begin{bmatrix} x^2 \\ x^2+1 \end{bmatrix} \leftrightarrow \begin{bmatrix} 0100 \\ 0101 \end{bmatrix} \leftrightarrow E$$

$d_{k_3}(Y_3) = K^{-1}Y_3$

$$= \begin{bmatrix} x^3+x+1 & x^3+x+1 \\ x^3+x^2 & x^2+1 \end{bmatrix} \begin{bmatrix} x^3 \\ x^3+x^2+x+1 \end{bmatrix} mod\ x^4+x+1$$

$$= \begin{bmatrix} x^2 \\ 0 \end{bmatrix} \leftrightarrow \begin{bmatrix} 0100 \\ 0000 \end{bmatrix} \leftrightarrow L$$

$d_{k_4}(Y_4) = K^{-1}Y_4$

$$=\begin{bmatrix} x^3+x+1 & x^3+x+1 \\ x^3+x^2 & x^2+1 \end{bmatrix}\begin{bmatrix} x^2 \\ x \end{bmatrix} mod\ x^4+x+1$$

$$=\begin{bmatrix} x^2 \\ x^3+1 \end{bmatrix} \leftrightarrow \begin{bmatrix} 0100 \\ 1001 \end{bmatrix} \leftrightarrow I$$

$d_{k_5}(Y_5) = K^{-1}Y_5$

$$=\begin{bmatrix} x^3+x+1 & x^3+x+1 \\ x^3+x^2 & x^2+1 \end{bmatrix}\begin{bmatrix} x^2 \\ x^2+1 \end{bmatrix} mod\ x^4+x+1$$

$$=\begin{bmatrix} x^2 \\ x^2+1 \end{bmatrix} \leftrightarrow \begin{bmatrix} 0100 \\ 0101 \end{bmatrix} \leftrightarrow E$$

$d_{k_6}(Y_6) = K^{-1}Y_6$

$$=\begin{bmatrix} x^3+x+1 & x^3+x+1 \\ x^3+x^2 & x^2+1 \end{bmatrix}\begin{bmatrix} x^2+1 \\ x \end{bmatrix} mod\ x^4+x+1$$

$$=\begin{bmatrix} x^2+1 \\ x^2+x \end{bmatrix} \leftrightarrow \begin{bmatrix} 0101 \\ 0110 \end{bmatrix} \leftrightarrow V$$

$d_{k_7}(Y_7) = K^{-1}Y_7$

$$=\begin{bmatrix} x^3+x+1 & x^3+x+1 \\ x^3+x^2 & x^2+1 \end{bmatrix}\begin{bmatrix} x^2 \\ x^2+1 \end{bmatrix} mod\ x^4+x+1$$

$$=\begin{bmatrix} x^2 \\ x^2+1 \end{bmatrix} \leftrightarrow \begin{bmatrix} 0100 \\ 0101 \end{bmatrix} \leftrightarrow E$$

Setelah Bob mendapatkan bloks-bloks plainteks yang disusun menjadi :$01000010 - 01000101 - 01000000 - 01001001 - 01000101 - 01010110 - 01000101$

- $01000010 \Longrightarrow 1000010 \leftrightarrow B$
- $01000101 \Longrightarrow 1000101 \leftrightarrow E$
- $01000000 \Longrightarrow 1000000 \leftrightarrow L$
- $01001001 \Longrightarrow 1001001 \leftrightarrow I$
- $01000101 \Longrightarrow 1000101 \leftrightarrow E$
- $01010110 \Longrightarrow 1010110 \leftrightarrow V$
- $01000101 \Longrightarrow 1000101 \leftrightarrow E$

Beberapa langkah perhitungan yang dilakukan oleh Bob, maka Bob berhasil membaca pesan rahasia dari Alice yaitu "BELIEVE" tanpa diketahui pihak ketiga.

Penyelesaian Masalah Menggunakan Program[5]

PROTOKOL PERJANJIAN KUNCI

```
>with(LinearAlgebra[Generic]); GF16 := GF(2, 4, x^4 + x + 1);
```

```
[BareissAlgorithm, BerkowitzAlgorithm, CharacteristicPolynomial,
    Determinant, GaussianElimination, GenericCheck,
    HermiteForm, HessenbergAlgorithm, HessenbergForm,
    LinearSolve, MatrixInverse, MatrixMatrixMultiply,
    MatrixVectorMultiply, MinorExpansion, NullSpace, RREF,
    ReducedRowEchelonForm, SmithForm,
    StronglyConnectedBlocks ]

GF16 := Z2[x] /` <x^4 + x + 1>
>print(GF16):
Z2[x] /` <x^4 + x + 1>
>R := Matrix([[x, 1], [1, x]]);
```

$$R := \begin{bmatrix} x & 1 \\ 1 & x \end{bmatrix}$$

```
>R := map(GF16:-ConvertIn, R);
```

$$R := \begin{bmatrix} x \bmod 2 & 1 \bmod 2 \\ 1 \bmod 2 & x \bmod 2 \end{bmatrix}$$

```
>W := Matrix([[x^2, x], [1, x]]);
```

$$W := \begin{bmatrix} x^2 & x \\ 1 & x \end{bmatrix}$$

```
>W := map(GF16:-ConvertIn, W);
```

$$W := \begin{bmatrix} x^2 \bmod 2 & x \bmod 2 \\ 1 \bmod 2 & x \bmod 2 \end{bmatrix}$$

```
>Ri := MatrixInverse[GF16](R)
```

$$Ri := \begin{bmatrix} (x^2+1) \bmod 2 & (x^3+x+1) \bmod 2 \\ (x^3+x+1) \bmod 2 & (x^2+1) \bmod 2 \end{bmatrix}$$

```
>L1 := MatrixMatrixMultiply[GF16](Ri, W)
```

$$L1 := \begin{bmatrix} (x^3+x^2) \bmod 2 & (x^3+x^2+x+1) \bmod 2 \\ (x^3+x^2+x+1) \bmod 2 & (x^3+x^2+x+1) \bmod 2 \end{bmatrix}$$

```
>L := MatrixMatrixMultiply[GF16](L1, R)
```

$$L := \begin{bmatrix} x^2 \bmod 2 & 1 \bmod 2 \\ x \bmod 2 & x \bmod 2 \end{bmatrix}$$

PROSES **PEMBUATAN** **KUNCI>**

```
S := Matrix([[x^2, 1], [x, x]]);
    # Alice menerima matrik S yang dikirim oleh Bob
```

$$S := \begin{bmatrix} x^2 & 1 \\ x & x \end{bmatrix}$$

```
>S := map(GF16:-ConvertIn, S);
```

$$S := \begin{bmatrix} x^2 \bmod 2 & 1 \bmod 2 \\ x \bmod 2 & x \bmod 2 \end{bmatrix}$$

> $K1 := MatrixMatrixMultiply\,[GF16\,](Ri, S)$
#Alice menghitung kunci rahasia

$$K1 := \begin{bmatrix} x \bmod 2 & 0 \bmod 2 \\ 0 \bmod 2 & 1 \bmod 2 \end{bmatrix}$$

> $K := MatrixMatrixMultiply\,[GF16\,](K1, R)$
#Alice mendapatkan kunci rahasia K

$$K := \begin{bmatrix} x^2 \bmod 2 & x \bmod 2 \\ 1 \bmod 2 & x \bmod 2 \end{bmatrix}$$

>

III. SIMPULAN DAN SARAN

A. *Simpulan*

Secara garis besar sistem keamanan kriptografi, khususnya pada pembuatan kunci rahasia menggunakan protokol perjanjian kunci digeneralisasi dari struktur aljabar sebagai landasan matemati.Dalam penelitian ini, penulis mengaplikasikan grup perkalian ring polinomial modulo sebagai landasan utama dalam perhitungan sistem komunikasi untuk pembuatan kunci rahasia melalui perhitungan protokol perjanjian kunci rahasia. Perhitungan protokol perjanjian kunci ini digeneralisasikan dari grup perkalian modulo polinomial taktereduksi berderajat m yang dinotasikan $GF(p^m)^*$ atau $\mathbb{Z}_p[x]/(f(x))^*$, untuk mendapatkan sebuah kesepakatan kunci rahasia, yang selanjutnya diimplementasikan dalam grup matriks invertibel, sehingga dapat dibentuk himpunan kunci berupa matriks invertibel atas lapangan hingga dengan notasi $GL_n(\mathrm{GF}(p^m))$, sedangkan pada himpunan Cipherteks dan Plainteks dibuat dalam bentuk vektor kolom atas lapangan hingga $GL_n(\mathrm{GF}(p^m))$. Sedemikian sehingga grup matriks atas lapangan hingga ini merupakan grup siklik non-komutatif yang dapat dibuktikan melalui beberapa aksioma dari struktur aljabar yaitu grup. Selanjutnya himpunan kunci, cipherteks, dan plainteks digunakan pada komunikasi pesan rahasia.

Keamanan algoritma perjanjiann kunci protokol ini terletak pada masalah konjugasi dalam pembuatan kunci yaitu *Diberikan suatu grup* G *dan* $w, x \in G$. *Masalah konjugasi diberikan untuk menentukan* $a \in G$ *sedemikian hingga* $a^{-1}wa = x$. Langkah selanjutnya, setelah menghitung dan mendapatkan kunci rahasia menggunakan algoritma protokol perjanjian kunci maka kunci rahasia tersebut diimplementasikan pada sistem keamanan Cipher Hill antara dua pihak yang melakukan komunikasi pesan rahasia namun tidak dapat bertemu secara langsung. Sistem keamanan Cipher Hil ini merupakan sistem kriptografi simetris yang proses enkripsi dan dekripsinya menggunakan kunci yang sama.

B. *Saran*

Berdasarkan penelitian yang telah penulis lakukan, maka dapat disampaikan beberapa saran sebagai berikut :

1) Penelitian ini hanya dibatasi dengan cara perhitungan pada pembuatan kunci rahasia menggunakan protokol perjanjian kunci yang berdasarkan masalah konjugasi, diharapkan ada penelitian selanjutnya berdasarkan masalah yang lainnya atau perbandingan dari permasalahan-permasalahan dari protokol perjanjian kunci.
2) Penelitian ini hanya membahas gambaran kecil mengenahi implementasi dari struktur aljabar pada sistem kriptografi, sehingga dimungkinkan penelitian lebih mendalam tentang struktur aljabar yang digeneralisasikan pada sistem kriptografi.

ISBN. 978-602-73403-0-5

DAFTAR PUSTAKA

[1]Myasnikov Alexei, dkk. *Grup Based Criptoggrafi* . 2008. Birkhäuser Verlag. Berlin
[2]Buchman, Johanes. *Introduction to Cryptograpy* . 2000. Barkey, USA
[3]Menezes, Oorcshot, and Vanstone. *Handbook of Applied Cryptography*. 1996. CRC Press. Inc. USA
[4]Riyanto, M. Zaki. Protokol Perjanjian Kunci Berdasarkan Masalah Konjugasi Atas Grup Non-Komutatif .Yogyakarta : 2012. Seminar Nasional Universitas Negeri Yogyakarta.
[5]E. Klima , Richard. *Aplications of Abstract Algebra With MAPEL*. 2000. Boca Raton London New York Washington, D.C.